[19]中华人民共和国国家知识产权局

[51]Int.Cl⁷
H04Q 7/20

[12]发明专利申请公开说明书

[21]申请号 99125575.5

[43]公开日 2000年9月13日

[11]公开号 CN 1266341A

[22]申请日 1999.12.3 [21]申请号 99125575.5
[30]优先权
[32]1999.3.3 [33]KR [31]6891/1999
[71]申请人 LG情报通信株式会社
地址 韩国汉城市
[72]发明人 朴亨善

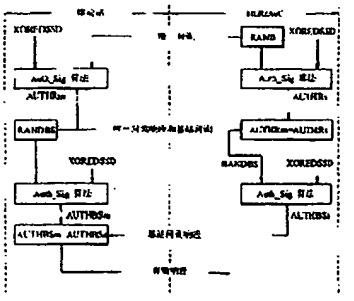
[74]专利代理机构 中原信达知识产权代理有限责任公司
代理人 余 朦 李 辉

权利要求书4页 说明书11页 附图页数5页

[54]发明名称 管理移动站操作参数的方法

[57]摘要

本发明披露了一种管理移动站操作参数的方法，其中执行移动站与网络之间的 相互鉴别。本发明的方法使得在保持常规的移动站操作参数更新程序的同时能够进行相互鉴别。



ISSN1008-4274

OCID: <CN 1266341A I >

权 利 要 求 书

1. 一种在无线通信网络中管理移动站操作参数的方法，包括：

从网络向移动站发送通知移动站操作参数更新开始的消息；和

在完成了移动站与网络间的相互鉴别后更新移动站操作参数。

2. 根据权利要求 1 所述的方法，其中响应通过移动站的使用者请求、通过网络的使用者请求中的一种，或响应移动站或网络特定状态期间的网络，发送所述消息。

3. 根据权利要求 1 所述的方法，其中更新移动站操作参数包括：

从网络向移动站发送至少一个移动站操作参数；和

更新所述至少一个存储在移动站中的移动站操作参数。

4. 根据权利要求 1 所述的方法，其中相互鉴别包括在移动站鉴别网络之前网络鉴别移动站。

5. 根据权利要求 4 所述的方法，其中相互鉴别包括：

在网络产生第一随机数并把第一随机数发送到移动站，和在网络利用第一随机数产生第一鉴别；

在移动站利用从网络接收的第一随机数产生第二鉴别并产生第二随机数，所述移动站把第二随机数连同第二鉴别发送到网络，并利用第二随机数产生第三鉴别；

把第二鉴别与第一鉴别比较；

在网络利用来自移动站的第二随机数产生第四鉴别；

如果第一鉴别和第二鉴别等价，从网络向移动站发送第四鉴别；

把第三鉴别与第四鉴别比较；和

如果第三鉴别与第四鉴别等价，那么完成一次相互鉴别。

6. 根据权利要求 5 所述的方法，其中连同所述消息一起向移动站

(CCID: <CN 1286341A 1 >

发送第一随机数。

7. 根据权利要求 5 所述的方法，其中在发送第二随机数和第二鉴别之前产生第三鉴别。

8. 根据权利要求 5 所述的方法，其中在把第二鉴别与第一鉴别比较之前产生第四鉴别。

9. 根据权利要求 4 所述的方法，其中相互鉴别包括：

在网络产生第一随机数并把第一随机数发送到移动站；

在移动站利用从网络接收的第一随机数产生第一鉴别和产生第二随机数，所述移动站把第二随机数连同第一鉴别发送到网络，并利用第二随机数产生第二鉴别；

在网络利用第一随机数产生第三鉴别，和把第三鉴别与来自移动站的第一鉴别比较；

在网络利用来自移动站的第二随机数产生第四鉴别；

如果第一鉴别与第二鉴别等价，向移动站发送第四鉴别；

把第二鉴别与第四鉴别比较；和

如果第二鉴别与第四鉴别等价，完成一次相互鉴别。

10. 根据权利要求 9 所述的方法，其中连同所述消息一起向移动站发送第一随机数。

11. 根据权利要求 9 所述的方法，其中在发送第二随机数和第一鉴别之前产生第二鉴别。

12. 根据权利要求 9 所述的方法，其中在比较第三鉴别与第一鉴别之前产生第四鉴别。

13. 根据权利要求 1 所述的方法，其中相互鉴别包括：移动站鉴

iOCID: <CN 1288341A I >

别网络在网络鉴别移动站之前进行。

14. 根据权利要求 13 所述的方法，其中相互鉴别包括：

在移动站产生第一随机数并利用第一随机数产生第一鉴别，所述移动站把第一随机数发送到网络；

在网络利用从移动站接收的第一随机数产生第二鉴别并产生第二随机数，所述网络把第二随机数连同第二鉴别发送到移动站并利用第二随机数产生第三鉴别；

比较第二鉴别与第一鉴别；

在移动站利用来自网络的第二随机数产生第四鉴别；

如果第一鉴别与第二鉴别等价，从移动站把第四鉴别发送到网络；

比较第三鉴别与第四鉴别；和

如果第三鉴别与第四鉴别等价，完成相互鉴别。

15. 根据权利要求 14 所述的方法，其中在发送第二随机数和第二鉴别之前产生第三鉴别。

16. 根据权利要求 14 所述的方法，其中在比较第二鉴别与第一鉴别之前产生第四鉴别。

17. 根据权利要求 13 所述的方法，其中相互鉴别包括：

在移动站产生第一随机数并把第一随机数发送到网络；

在网络利用从移动站接收的第一随机数产生第一鉴别并产生第二随机数，所述网络把第二随机数连同第一鉴别发送到移动站并利用第二随机数产生第二鉴别；

在移动站利用第一随机数产生第三鉴别，和比较第三鉴别与来自网络的第一鉴别；

在移动站利用来自网络的第二随机数产生第四鉴别；

如果第一鉴别和第二鉴别是等价的，把第四鉴别发送到网络；

比较第二鉴别与第四鉴别；和

如果第二鉴别与第四鉴别是等价的，完成相互鉴别。

18. 根据权利要求 17 所述的方法，其中在发送第二随机数和第一鉴别之前产生第二鉴别。

19. 根据权利要求 17 所述的方法，其中在比较第三鉴别与第一鉴别之前产生第四鉴别。

20. 一种执行 OTAPA 程序的方法，包括：

确定移动站是否可用于 OTAPA；

如果移动站可用于 OTAPA，在网络产生并存储第一随机数；

向移动站发送一个通知 OTAPA 程序开始的消息以及第一随机数；

在移动站利用第一随机数产生第一鉴别，第二随机数，和第二鉴别；

向网络发送一个响应消息以及第二随机数和第一鉴别；

在网络通过利用第一随机数产生第三鉴别、并比较第一鉴别与第三鉴别来开始鉴别程序；

如果第一鉴别与第三鉴别等价，利用第二随机数产生并发送第四鉴别；

在移动站比较第四鉴别与第二鉴别，并且如果等价，向网络发送允许参数更新的第二消息；

一旦接收到第二消息，从网络向移动站发送至少一个用于更新的参数；和

在移动站更新所述至少一个用于更新的参数。

IOCID: <CN 1286341A I >

说　明　书

管理移动站操作参数的方法

本申请的优选权申请是 1999 年 3 月 3 日提交的第 P99-6891 号韩国专利申请，在这里完整地引用该专利申请作为参考。

本发明涉及一种移动通信系统，更具体地讲，是涉及在移动通信系统中管理移动站操作参数的方法。在本发明中，以适当的方式管理移动站的操作参数，使得在保持同样数量的操作参数更新的同时，可以执行移动站与网络间的相互鉴别。

由于信息和通信领域中的迅速发展，基于蜂窝或个人通信系统（PCS）的移动通信网正在持续地扩展。因此，移动通信网络的各种功能被不断地更新，以便为用户提供更为便利的通信服务。

为了更新特定网络功能，网络管理者必须改变安装在基站（BS），基站控制器（BSC），移动交换中心（MSC），原始/访问者位置寄存器（HLR/VLR），和鉴别中心之类的通信装置中的程序和操作参数。此外，网络管理者也必须改变每个移动站中的特定参数。但是，为了改变移动站中特定参数，必须把移动站物理地连接到能够改变这些参数的系统上，或使用者必须正确地手动操作移动站的键盘。

因此，已经发展了一种允许通过无线通信来改变移动站的特定参数的技术，称为越空参数管理（Over-The-Air Parameter Administration(OTAPA)）。OTAPA 由北方电信公司（Northern Telecom Inc.）于 1999 年 4 月 13 日发表在 IS-725-A 的第 1-19 和 3-75 到 3-78 页中，或第 WO 98/41044 号 PCT 申请中，本发明完全结合该项技术。

根据 IS-725-A，对于一个通信网络的鉴别程序包括在 OTAPA 处

理中，因而使得移动站可以确认网络是否正确，但是并不包括对移动站的鉴别程序。结果，一个人可以非法地改变移动站的特定参数，和非法地接收通信服务，因而影响对网络的合法使用者，即，移动站的整体服务。因此，可能会降低网络合法使用者的管理系统可靠性，并且也可能破坏服务质量。

尽管在 OTAPA 处理之前网络可以首先进行移动站的鉴别程序，但是，如果移动站的鉴别程序是独立进行的，将会使整个 OTAPA 处理时间延长。此外，必须增加一个独立的鉴别程序，因而增加了通信网络的负担。

因此，本发明的目的是至少要解决现有技术的问题和缺陷。

本发明的一个目的是要使进行移动站与网络间的相互鉴别的管理成为可能。

本发明的另一个目的是要使在保持如同现有程序一样的移动站操作参数更新数量的同时，进行移动站与网络间的相互鉴别的管理成为可能。

在以下的说明中将部分地提出本发明的附加优点、目的和特征，本领域普通技术人员通过审查以下的说明，或通过实践本发明，可部分地了解它们。可以如附属的权利要求中特别指出的那样实现和达到本发明的目的和优点。

为达到这些目的并根据本发明的意图，作为这里的具体体现和广义的说明，一种在无线通信网络中管理移动站操作参数的方法包括：在从移动站请求更新时，通知移动站移动站操作参数更新已经开始；执行移动站与网络间的相互鉴别程序；从网络向移动站发送至少一个移动站操作参数；和在移动站接收并更新相应的移动站操作参数。

OCID: <CN 1266341A I >

相互鉴别还可以包括：从网络产生并向移动站发送第一随机数，并利用第一随机数产生第一鉴别；在移动站利用第一随机数产生第二鉴别和第二随机数，并把第二随机数连同第二鉴别发送到网络，然后利用第二随机数产生第三鉴别；在网络把第二鉴别与第一鉴别相比较，并鉴别移动站；当第一鉴别与第二鉴别等价时，在网络利用第二随机数产生第四鉴别，并向移动站发送第四鉴别；在移动站把第三鉴别与第四鉴别相比较，并根据比较结果鉴别网络。

相互鉴别还可以包括：在移动站产生第三随机数并发送到网络，并利用第三随机数产生第五鉴别；在网络利用第三随机数产生第六鉴别和第四随机数，并把第四随机数连同第六鉴别发送到移动站，然后利用第四随机数产生第七鉴别；在移动站把第五鉴别与第六鉴别相比较，并在移动站根据比较结果鉴别网络；当第五与第六鉴别等价时，在移动站利用第四随机数产生第八鉴别，并把第八鉴别发送到网络；在网络比较第七鉴别与第八鉴别，并根据比较结果鉴别移动站。

以下参考附图对本发明进行详细的说明，在附图中相同的元件使用了相同的参考号，其中：

图 1 和 2 是说明根据本发明的第一实施例的移动站与网络间相互鉴别程序的时序图；

图 3 是说明根据本发明第一实施例的详细 OTAPA 处理的时序图；

图 4 和 5 是说明根据本发明的第二实施例的移动站与网络间相互鉴别程序的时序图。

为执行 OTAPA，在每个移动站和无线通信网络的每个元件中执行各种功能。

移动站和网络都必须有在需要时内部产生随机数的能力，并且必

YCIP-CN 1269341A

须存储保密关键码（A_KEY）以及共享保密数据（SSD）。A_KEY 是一种存储在移动站和原始位置寄存器（HLR）或鉴别中心（AC）中的 64 位模式。用它产生或更新移动站的 SSD。SSD 是存储在移动站中，并为基站所知的一种 128 位模式。并且，HLR 必须知道每个移动站支持 OTAPA 功能。

OTAPA 程序一般可以划分为四个部分。首先，网络响应使用者手动操作移动站上的键盘而通过移动站发出的请求、通过网络的使用者的请求、或是在移动站或网络的特定状态期间响应网络，将移动站操作参数更新的开始通知移动站。在本发明中，网络包括移动交换中心和鉴别中心（AC）之间的元件。

其次，执行移动站与网络之间的相互鉴别程序。在鉴别程序中，网络可以首先鉴别移动站，然后移动站可以鉴别网络；或者移动站可以首先鉴别网络，然后网络可以鉴别移动站。

图 1 和 2 说明了相互鉴别程序的第一实施例，其中网络鉴别移动站先于移动站鉴别网络。

参考图 1 和 2，如图 2 的 a2 所示，网络产生第一随机数 RAND，并利用 OTAPA 请求消息请求来自移动站 MS 的唯一问询指令（challenge order）。在 OTAPA 消息中可以包括一个通知移动站操作参数更新开始的消息。网络还利用第一随机数 RAND 产生第一鉴别 AUTHRs。

移动站 MS 接收来自网络的第一随机数 RAND，并利用第一随机数 RAND 产生第二鉴别 AUTHRm。移动站进一步产生第二随机数 RANDBS，并将其连同第二鉴别 AUTHRm 发送到网络。因而，如图 2 的 b2 和 c2 所示，移动站产生了一个唯一问询响应，并且利用 OTAPA 响应通过网络的一个基站 BS 或 MSC/OTAPA 请求向一个 HLR 或 AC

OCID: <CN 1286341A I >

的一个基站问询指令。然后，移动站 MS 利用第二随机数 RANDBS 产生第三鉴别 AUTHBSm。

在上述情况中，第三鉴别 AUTHBSm 是在第二随机数 RANDBS 和第二鉴别 AUTHRm 发送之后产生的。但是，移动站可以在第二随机数 RANDBS 和第二鉴别 AUTHRm 发送之前产生第三鉴别 AUTHBSm。

在接收到来自移动站 MS 的发送之后，网络的 HLR/AC 把第二鉴别 AUTHRm 与网络中产生的第一鉴别 AUTHRs 比较。如果第一鉴别 AUTHRs 与第二鉴别 AUTHRm 等价，那么如图 2 的 e2 所示，网络利用第二 RANDBS 产生第四鉴别 AUTHBSs，并通过一个有效请求（validation request）把第四鉴别 AUTHBSs 发送到移动站 MS。在这里网络可以首先产生第四鉴别 AUTHBSs，然后再根据上述比较发送第四 AUTHBSs。

移动站 MS 接收来自网络的第四 AUTHBSs，并且把第三 AUTHBSm 与第四 AUTHBSs 比较。如果两个鉴别 AUTHBSm 和 AUTHBSs 等价，那么如图 2 的 f2 所示，移动站 MS 通过一个有效响应向网络发送一个指示相互鉴别已成功执行的消息。

在上面说明的相互鉴别程序中，移动站可以产生第一鉴别。在这种情况下，网络将产生和存储第一随机数 RAND，并向移动站 MS 发送第一随机数 RAND。当接收到第一随机数 RAND 后，移动站 MS 将利用网络发送的第一随机数 RAND 产生第一鉴别，和产生第二随机数 RANDBS，并将其连同第一鉴别发送到网络。接下来移动站 MS 将利用第二随机数 RANDBS 产生第二鉴别。

因此，网络将利用第一随机数 RAND 产生第三鉴别，并且把第一鉴别与第三鉴别比较，以鉴别移动站 MS。如果第一和第三鉴别等价，

那么网络将利用第二随机数 RANDBS 产生第四鉴别，并将第四鉴别发送给移动站 MS。

在上述情况中，移动站可以在第二随机数 RANDBS 和第一鉴别发送之前产生第二鉴别。网络也可以首先产生第四鉴别，然后根据比较的结果发送第四鉴别。

因此，移动站 MS 将通过比较第四和第二鉴别来鉴别网络，并且如果成功地执行了相互鉴别，网络向移动站 MS 发送需要的参数值。最后，移动站 MS 接收该参数值并更新旧参数。

图 3 是说明根据本发明实施例的 OTAPA 处理的抽样时序图，其中移动站产生第一鉴别。参考图 3，如图 3 的 a3 和 b3 所示，当由于通过 MS 10 或网络的使用者请求，或由于 MS 10 或网络的特定状态，需要改变移动站 MS 10 的操作参数时，网络的越空服务提供功能（Over-The-Air Service Provisioning Function）（OTAF）40 查询 HLR 50，以确定 MS 10 是否可用于 OTAPA。

根据本发明，在请求移动站 MS 10 的短消息服务（SMS）的操作中，或是在请求用于 OTAPA 功能的位置信息的 OTAPA 程序中使用 SMSRequest(SMSREQ)。服务标志（SRVIND）用于确定服务选择为 OTA 服务提供（OTA Service Provisioning）（OTASP）还是 OTAPA。smsreq 是 SMSREQ 的响应消息。一般用大写字母表示指示操作开始的消息，而用小写字母代表对该操作的响应消息。

如果 MS 10 可以执行 OTAPA，OTAF 40 产生并存储要在鉴别处理中使用的随机数 RAND。OTAF 40 还通过 c3 中所示的消息向 MS 10 通知 OTAPA 程序的开始。具体地讲，OTAF 40 把随机数 RAND 连同消息 SMSDclivery Point To Point(SMDPP)一起发送。

IOCID: <CN 1266341A I >

如 IS-683-A 中所定义的，在 SMS 的短消息的传输中和 MS 10 与 OTAF 40 之间的消息传输中使用 SMDPP。ActionCode(ACTCODE)是在更新内容的确定中使用的参数，SMS_BearerData 是用于在 MS 10 与 OTAF 40 之间发送消息的参数。

接下来，MS 10 接收来自 OTAF 40 的随机数 RAND，并利用共享保密数据 SSD 和保密关键码 A_KEY 通过"异"操作产生 XOREDSSD。MS 10 利用 XOREDSSD，还使用已经存储在其中的移动标识号（MIN）和电序号（ESN），产生一个鉴别 AUTHR。然后，MS 10 产生一个用于鉴别网络的新的随机数 RAND_OTAPA，并利用 RAND_OTAPA、XOREDSSD、MIN 和 ESN 产生一个新的鉴别 AUTH_OTAPA。

具体地讲，AUTHR 是利用存储在 MS 10 中的保密关键码 A_KEY，随机数 RAND 和 MIN 通过执行一种鉴别算法获得的。如果是网络产生第一鉴别，那么第一鉴别利用存储在 AC 60 中的保密关键码 A_KEY，随机数 RAND 和 MIN 通过执行鉴别算法获得。在这里，MIN 是一个 40 位数，是分配给一个移动站的 10 位十进制号码的数字表示。ESN 是移动站制造商赋予的，用来唯一地标识移动站设备的一个 32 位数。

因而，如图 3 的 e3 所示，MS 10 向 OTAF 40 发送带有随机数 RAND_OTAPA 的响应消息，和利用来自 OTAF 40 的随机数 RAND 产生的鉴别 AUTHR。在这里，Smdpp 是 SMDPP 消息的响应消息，RAND_OTAPA（随机 OTAPA）是一个随机数，NAM 锁定标志（NAM_LOCK_IND）是一个指示是否保护参数更新的参数。

接下来，OTAF 40 接收从 MS 10 发送的 OTAPA 响应消息。如果 OTAF 40 确定 NAM 被保护，那么 OTAF 40 通过把接收的随机数 RAND_OTAPA 转换为随机数 RANDBS 开始鉴别程序。然后，如 f3 和 g3 中所示，OTAF 40 向 AC 60 发送随机数 RANDBS，鉴别 AUTHR

和随机数 RAND。OTASPREQ 是 OTAF 40 开始鉴别程序所使用的一个参数。

在接收到随机数 RAND 和 RANDBS 以及鉴别 AUTHR 后，AC 60 利用随机数 RAND，XOREDSSD，MIN 和 ESN，通过参考 MS 10 描述的相同的算法再次产生鉴别 AUTHR。因此，AC 60 把内部产生的鉴别 AUTHR 与从 MS 10 接收的鉴别 AUTHR 相比较。如果两个鉴别等价，那么如 h3 和 i3 中所示，AC 60 产生第四鉴别 AUTHBS，并且向 OTAF 40 发送第四鉴别 AUTHBS，以及产生的 XOREDSSD，MIN，ESN。在这里，鉴别响应基站问询（Authentication Response Base Station Challenge）（AUTHBS）等价于鉴别 AUTHR，但是代表在基站问询过程中获得的一个鉴别值。

然后，把网络中利用的鉴别 AUTHBS 转换为鉴别 AUTH_OTAPA，一种在 MS 10 与 OTAF 40 间发送或接收使用的格式。因而，如 h3 和 j3 中所示，OTAF 40 接收来自 AC 60 的一个消息中的鉴别 AUTHBS，并把鉴别 AUTHBS 转换为鉴别 AUTH_OTAPA。把转换后的鉴别 AUTH_OTAPA 发送到 MS 10。

MS 10 接收来自 OTAF 40 的鉴别 AUTH_OTAPA，并把接收的鉴别 AUTH_OTAPA 与内部产生的鉴别 AUTH_OTAPA 相比较。如果两个鉴别 AUTH_OTAPA 等价，那么 MS 10 识别出成功地执行了 MS 10 和网络之间的相互鉴别。因此，如 l3 中所示，MS 10 向 OTAF 40 发送一个允许参数更新程序的消息。

此后，如 m3 至 o3 中所示，OTAF 40 向 MS 10 发送需要的参数，并且如果适合，那么如 q3 中所示，还发送一个存储参数的指令消息。一旦接收到来自 OTAF 40 的存储指令，如 r3 和 s3 中所示，MS 10 用新接收的参数更新或改变旧的参数，并向 OTAF 40 发送指示参数成功更新的消息。最后，如 t3 至 v3 中所示，OTAF 40 向 MS 10 发送一个

指示整个鉴别程序完成的消息。

图 4 和 5 示出了说明根据本发明的第二实施例的移动站与网络间相互鉴别程序的时序图。

参考图 4 和 5，如图 5 的 a5 所示，网络向移动站 MS 发送通知 OTAPA 开始的消息。通知 OTAPA 开始的消息可以包括在 OTAPA 消息中。接收到消息后，移动站 MS 产生第一随机数 RANDBS，并利用随机数 RANDBS 产生第一鉴别 AUTHBSm。如图 5 的 b5 和 c5 中所示，移动站 MS 也通过 OTAPA 响应向网络发送随机数 RANDBS。

网络接收随机数 RANDBS，并利用随机数 RANDBS 产生第二鉴别 AUTHBSs。网络还产生在移动站 MS 的鉴别中使用的随机数 RAND，并利用随机数 RAND 产生第三鉴别 AUTHRs。然后，如图 5 的 d5 和 e5 所示，网络把产生的鉴别 AUTHBSs 连同随机数 RAND 发送到移动站 MS。如同本发明的第一实施例一样，第三鉴别 AUTHRs 可以在第二鉴别 AUTHBSs 和随机数 RAND 发送之前或之后产生。

一旦接收到鉴别 AUTHBSs 和随机数 RAND，移动站 MS 把鉴别 AUTHBSs 与内部产生的鉴别 AUTHBSm 相比较，以便鉴别网络。如果两个鉴别 AUTHBSs 和 AUTHBSm 等价，那么移动站 MS 利用来自网络的随机数 RAND 产生第四鉴别 AUTHRm。因而，如图 5 的 f5 所示，移动站 MS 通过唯一问询响应消息把产生的鉴别 AUTHRm 发送到网络。在这里同样是，移动站 MS 可以首先产生第四鉴别 AUTHRm，然后根据比较的结果发送第四鉴别 AUTHRm。

接下来，网络通过唯一问询响应接收来自移动站 MS 的鉴别 AUTHRm，并把鉴别 AUTHRm 与内部产生的鉴别 AUTHRs 相比较。如果两个鉴别 AUTHRs 和 AUTHRm 等价，那么成功地执行了移动站 MS 的鉴别。因此，完成了其中移动站 MS 鉴别网络先于网络鉴别移动

站 MS 的相互鉴别。

在相互鉴别程序的第二实施例中，网络也可以产生第一鉴别。在这种情况下，移动站 MS 产生和存储第一随机数 RANDBS，并向网络发送第一随机数 RANDBS。当接收到第一随机数 RANDBS 时，网络利用移动站 MS 发送的第一随机数 RANDBS 产生第一鉴别，并产生第二随机数 RAND，并把第二随机数 RAND 连同第一鉴别发送到移动站 MS。网络接下来利用第二随机数 RAND 产生第二鉴别。

然后，移动站 MS 利用第一 RANDBS 产生第三鉴别，并把第一鉴别与第三鉴别比较，以便鉴别网络。如果第一和第三鉴别等价，那么移动站 MS 利用第二随机数 RAND 产生第四鉴别，并把第四鉴别发送到网络。

在上述情况中，网络可以在第二随机数 RAND 和第一鉴别发送之前产生第二鉴别。移动站 MS 也可以首先产生第四鉴别，然后根据比较结果发送第四鉴别。

因此，网络将通过比较第四和第二鉴别来鉴别移动站 MS，并且如果成功地执行了相互鉴别，网络向移动站 MS 发送需要的参数值。最后，移动站 MS 接收参数值并更新旧参数。此外，OTAPA 程序是以与参考本发明的第一实施例说明的相同方式执行的。

总之，根据本发明，移动站 MS 和网络间相互鉴别可以在现有技术的 OTAPA 程序内执行。因此，本发明使得非法移动站使用者难于不正常地或非法地改变移动站操作参数。结果，本发明使得无线通信网络公司能够提高移动站的合法预约可用性，因而提高了服务质量和管理网络的可靠性。

上述实施例仅是示例性的，并不构成对本发明的限制。本发明可

CCID-CN 1266341A

以容易地应用于其它类型的装置。本发明的说明只是用来解释，并不限制权利要求的范围。熟悉本领域的人员应当知道可以有许多替代、修改和改变。

图1

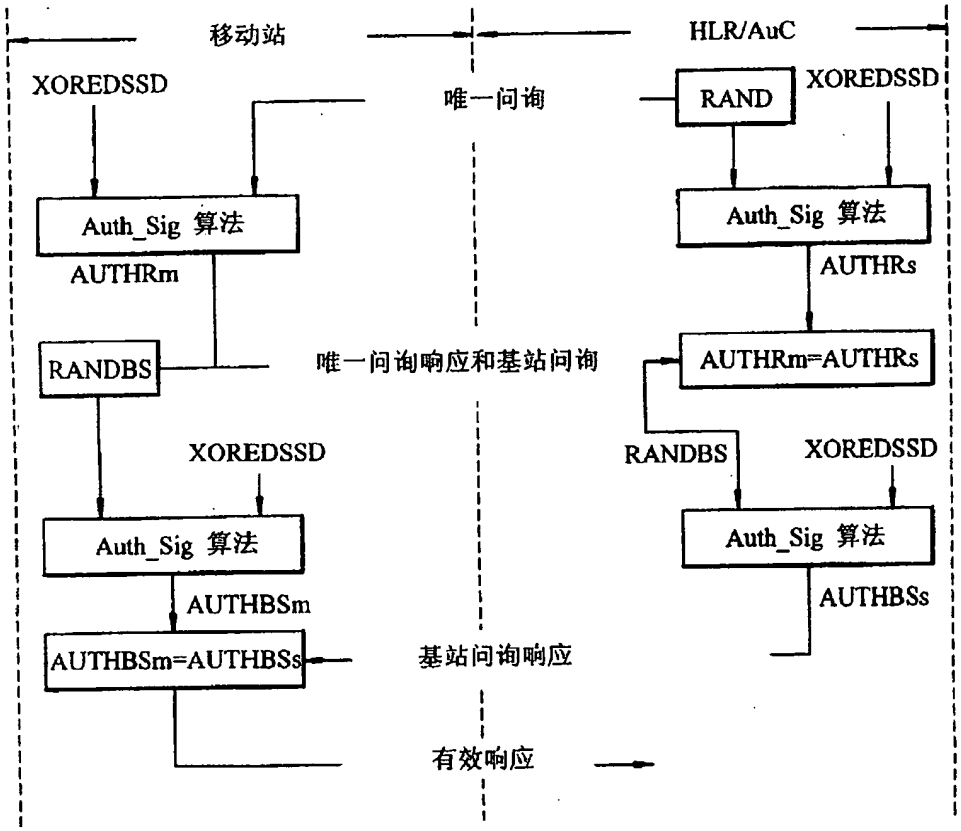

移动站
HLR/AuC
XOREDSSD
唯一问询
RAND
XOREDSSD
Auth_Sig 算法
Auth_Sig 算法
AUTHRm
AUTHRs
RANDBS
唯一问询响应和基站问询
AUTHRm=AUTHRs
XOREDSSD
RANDBS
XOREDSSD
Auth_Sig 算法
Auth_Sig 算法
AUTHBSm
AUTHBSs
AUTHBSm=AUTHBSs
基站问询响应
有效响应

图2

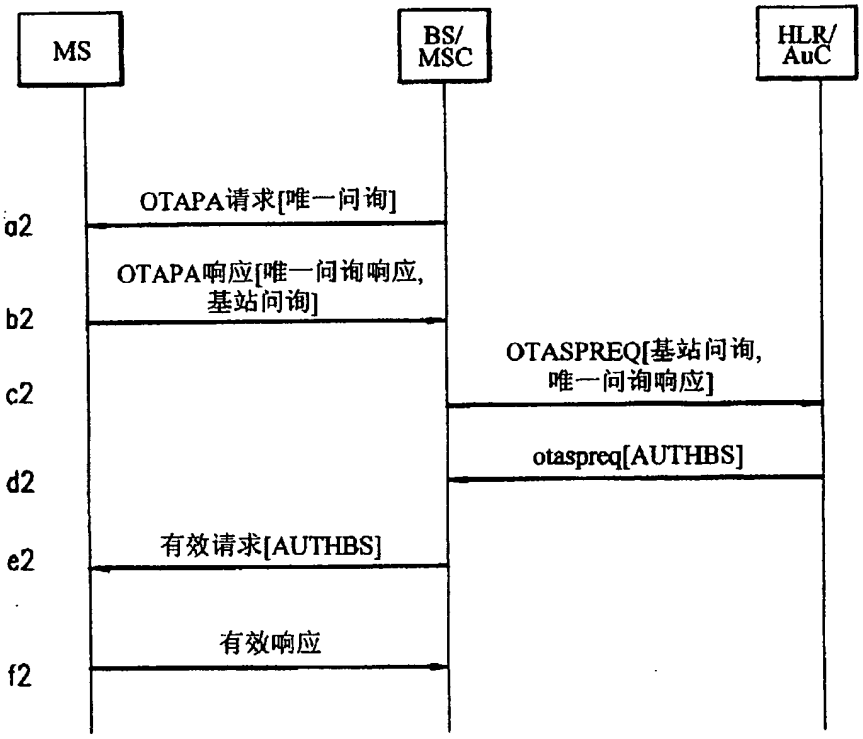

MS
BS/
MSC
HLR/
AuC
a2
OTAPA请求[唯一问询]
b2
OTAPA响应[唯一问询响应,
基站问询]
c2
OTASPREQ[基站问询,
唯一问询响应]
d2
otaspreq[AUTHBS]
e2
有效请求[AUTHBS]
f2
有效响应

图3

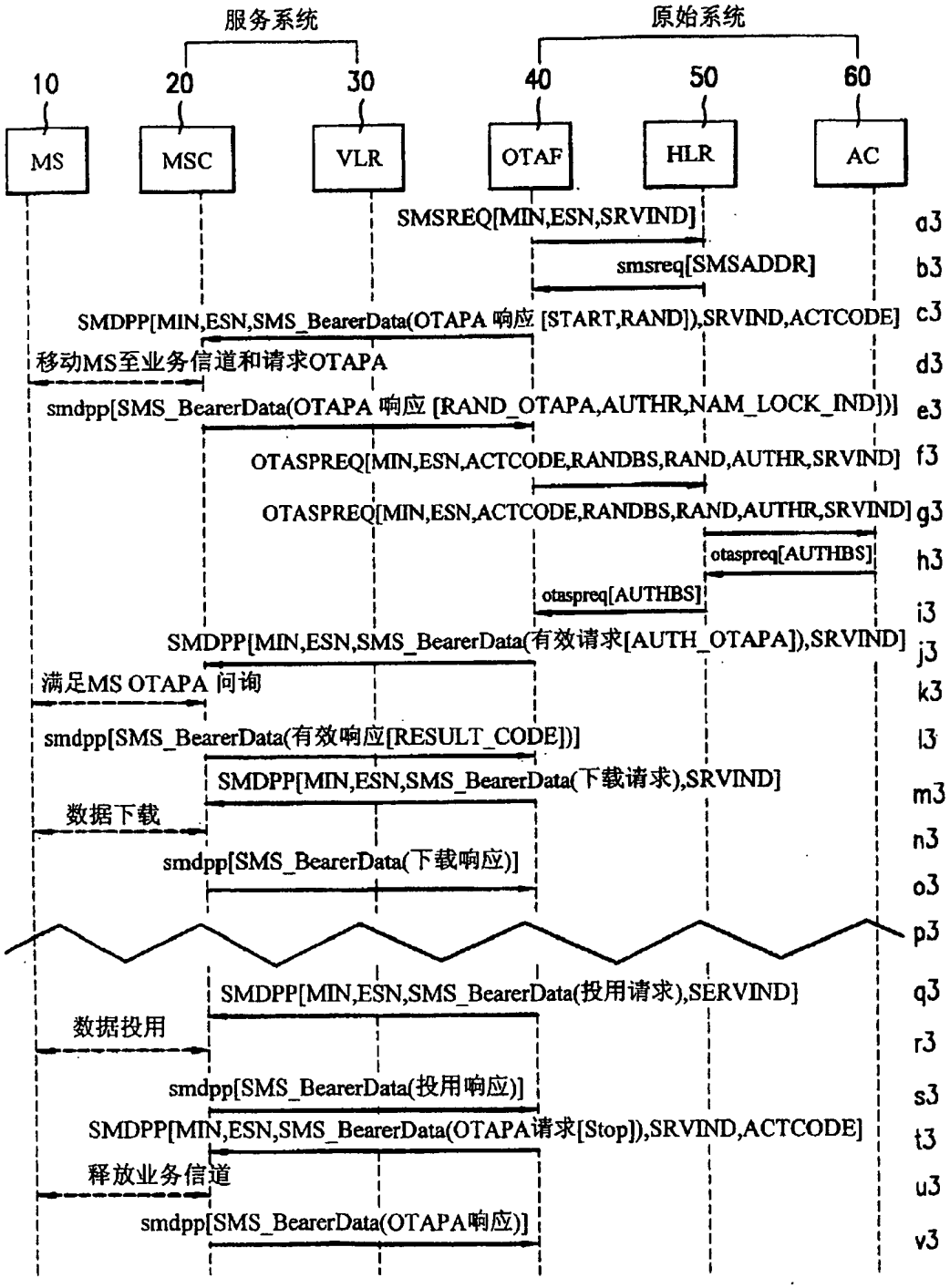

服务系统
原始系统
10
20
30
40
50
60
MS
MSC
VLR
OTAF
HLR
AC
SMSREQ[MIN,ESN,SRVIND]
a3
smsreq[SMSADDR]
b3
SMDPP[MIN,ESN,SMS_BearerData(OTAPA 响应 [START,RAND]),SRVIND,ACTCODE]
c3
移动MS至业务信道和请求OTAPA
d3
smdpp[SMS_BearerData(OTAPA 响应 [RAND_OTAPA,AUTHR,NAM_LOCK_IND])]
e3
OTASPREQ[MIN,ESN,ACTCODE,RANDBS,RAND,AUTHR,SRVIND]
f3
OTASPREQ[MIN,ESN,ACTCODE,RANDBS,RAND,AUTHR,SRVIND]
g3
otaspreq[AUTHBS]
h3
otaspreq[AUTHBS]
i3
SMDPP[MIN,ESN,SMS_BearerData(有效请求[AUTH_OTAPA]),SRVIND]
j3
满足MS OTAPA 问询
k3
smdpp[SMS_BearerData(有效响应[RESULT_CODE])]
l3
SMDPP[MIN,ESN,SMS_BearerData(下载请求),SRVIND]
m3
数据下载
n3
smdpp[SMS_BearerData(下载响应)]
o3
p3
SMDPP[MIN,ESN,SMS_BearerData(投用请求),SERVIND]
q3
数据投用
r3
smdpp[SMS_BearerData(投用响应)]
s3
SMDPP[MIN,ESN,SMS_BearerData(OTAPA请求[Stop]),SRVIND,ACTCODE]
t3
释放业务信道
u3
smdpp[SMS_BearerData(OTAPA响应)]
v3

图4

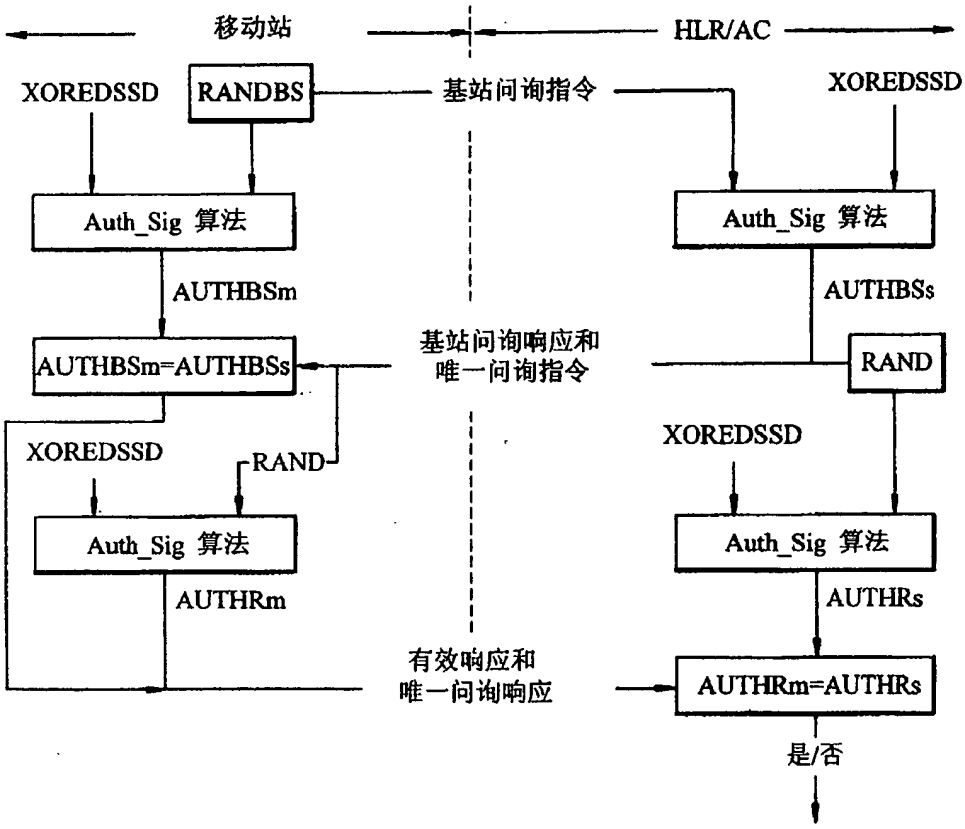
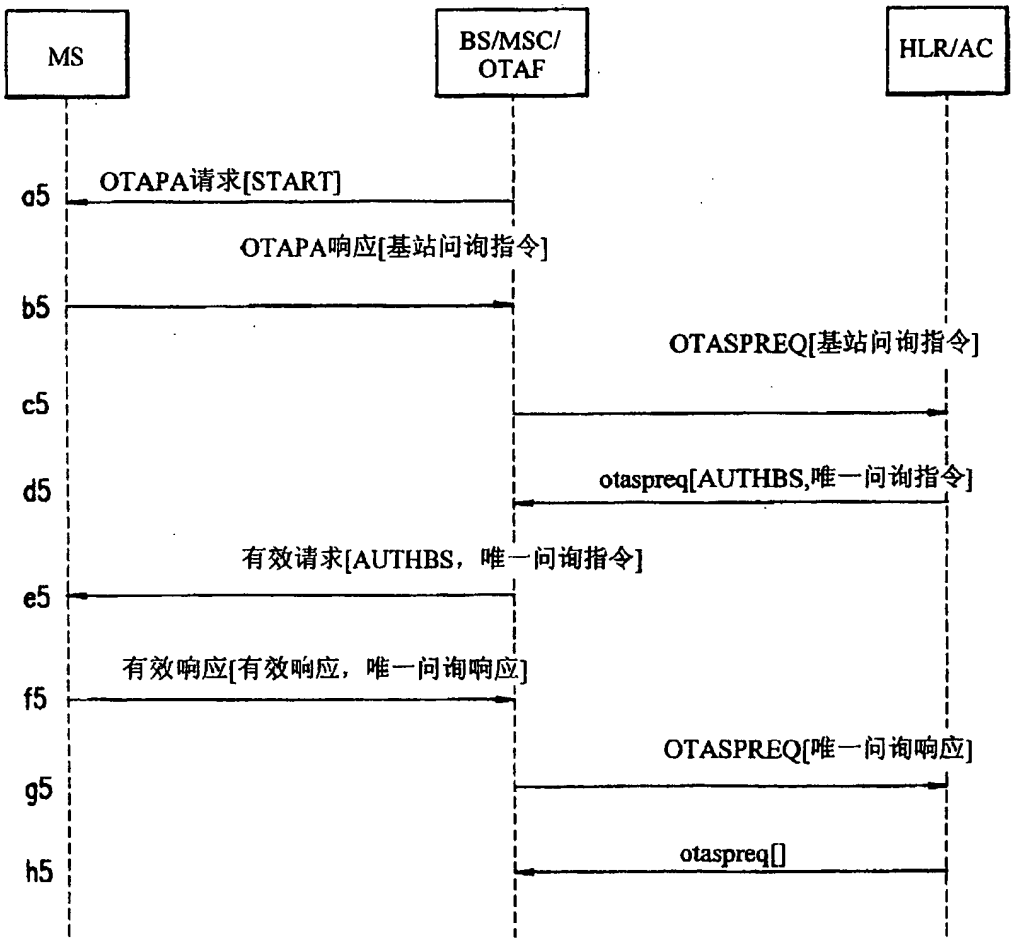

移动站
HLR/AC
XOREDSSD
RANDBS
基站问询指令
XOREDSSD
Auth_Sig 算法
Auth_Sig 算法
AUTHBSm
AUTHBSs
AUTHBSm=AUTHBSs
基站问询响应和
唯一问询指令
RAND
XOREDSSD
XOREDSSD
RAND
Auth_Sig 算法
Auth_Sig 算法
AUTHRm
AUTHRs
有效响应和
唯一问询响应
AUTHRm=AUTHRs
是/否

图5



DCID: <CN___1288341A_I_>